CVFG@GR A

# DECLARATION OF JULIAN ACKERT

I, Julian Ackert, hereby declare as follows:

## Background and Professional Qualifications

1. I am a Managing Director at iDiscovery Solutions, Inc., ("iDS"), an expert services and consulting firm that provides independent computer forensics, electronic discovery expert testimony and analysis, original authoritative studies, and strategic consulting services to the business and legal community.

2. I have over 20 years of experience in consulting and litigation technologies that focus on electronic discovery and computer forensics. I have a Bachelor of Science degree in Computer Science from the University of Virginia. My curriculum vitae is attached hereto as Exhibit A, which details my professional experience and all articles and testimony I have completed over the last ten years.

3. Specifically, I have extensive experience creating and implementing preservation, collection, and production strategies and performing computer forensics and metadata analysis on electronically stored information ("ESI"). I have performed preservation, collection, analysis, and production of ESI in hundreds of matters.

4. This declaration is based on my knowledge, years of experience, training, education, and the information provided to date. The opinions provided herein are given to a reasonable degree of professional certainty.

5. My forensic analysis and testimony rate is $625 per hour, and iDS is also being reimbursed for reasonable expenses and the cost of other employees working under my supervision. My opinions are not contingent on fees earned by iDS in this matter.

6. When I state “I,” “Myself,” or “iDS,” I mean this work was done by me or by people

working at my direction and supervision within iDS.

**Assignment**

7. I was retained by Greenberg Traurig, on behalf of Middesk, Inc. ("Middesk"), to analyze the Middesk computer and activity logs of former employee Josh Leviloff ("Leviloff"), to investigate concerning activity prior to his departure, and to understand whether Leviloff took, deleted, and/or still possesses Middesk data. I was advised that Leviloff's last day of employment with Middesk was February 21, 2025.

**Assumptions**

8. I was asked to use the following assumptions in forming my opinions.

   a. Leviloff's last day of employment with Middesk was February 21, 2025.

   b. Before February 21, 2025, Leviloff accepted employment with Baselayer, which I understand is a competitor of Middesk.

   c. Jonathan Awad ("Awad"), Baselayer's founder, was formerly employed by Middesk.

**Summary of Opinions and Findings**

9. As of February 20, 2025, Leviloff downloaded or synchronized at least 38 files from Middesk's Google Drive to a device other than his Middesk laptop. Based on the review of filenames, the files downloaded include files related to Middesk's pricing, business operations, and sales pipeline.

10. On February 21, 2025, the last day of his employment with Middesk, Leviloff's Internet browsing history was cleared on his Middesk laptop, which limited my ability to conduct a full forensic investigation into the Internet browser activity. The browsing history was cleared by the user logged into the Middesk laptop account at the time.

11. Despite this, I determined that Leviloff's Middesk Laptop:

a. Was used to access his personal Gmail account, jXXXXXXXXX@gmail.com;[1] and

b. Accessed multiple Middesk Salesforce website "pages", including those that appear to be related to Middesk sales pipeline, pricing, and accounts.

12. Starting on December 5, 2024, Leviloff began accessing the Middesk Salesforce system from an iPhone. This Middesk Salesforce system access from an iPhone continued through February 21, 2025. In order to fully determine the Middesk Salesforce system data that was accessed from and/or downloaded to the iPhone, I would need to examine the iPhone.

13. On the Leviloff Middesk laptop, there is evidence of text message communications between Leviloff and Awad related to Leviloff's future employment at Baselayer in the text message database. Because Leviloff disconnected his text message database from his Middesk laptop on approximately February 6, 2025, the full extent of these communications, including any communications sent or received after February 6, 2025, cannot be determined without access to additional information such as the Leviloff iCloud account text message database.

14. The laptop previously assigned to Awad while he was employed at Middesk is linked to a personal Apple ID account (j*****@gmail.com)[2] and cannot be accessed or analyzed without access to the Apple ID and password.

15. Based on my experience in conducting similar investigations, I will need access to additional devices and accounts, described in detail further below, to determine the full

[1] For the purposes of this declaration, I have masked the actual email address.

[2] The email address is obscured on the screen of the Awad Laptop, indicating that the computer is linked to this account. One must type the full email address and password to gain access.

extent of storage, transfer, or conveyance of Middesk information outside of Middesk's accounts and devices. Because a laptop and computer activity logs do not record all activity related to data copies and/or uploads to other devices and accounts, my findings should be considered the floor of Middesk data exfiltration activity and not the ceiling.

16. The details of my analysis, including the items which I reviewed, along with my methodology and tools are described below.

**Materials Reviewed**

17. During my analysis, I reviewed the following materials:

a. Forensic image of an Apple MacBook Pro 14" Laptop, model A2779, serial number J9P7DVQ0NL, Middesk asset number MD00106, assigned by Middesk to Josh Leviloff ("Leviloff Laptop"),

b. Google Drive audit logs for the account jleviloff@middesk.com, exported and provided by Middesk ("Google Drive Logs"),

c. Salesforce login activity logs for Josh Leviloff's account, exported and provided by Middesk ("Salesforce Login Logs"),

d. Slack messages, in Excel format, involving user **joshleviloff**, exported and provided by Middesk ("Slack Messages").

e. Apple MacBook Pro 13", serial number FVFH705Q0KPF, previously assigned by Middesk to Awad ("Awad Laptop").

**Tools**

18. iDS used the following tools in its analysis:

a. Cellebrite Digital Collector v3.8

b. mac_apt v1.7.5 (dev)

c. Magnet Forensics Axiom v8.9.1.43258

d. DB Browser for SQLite v3.12.2

e. Microsoft® Excel® for Microsoft 365 MSO (Version 2502 Build 16.0.18526.20168) 64-bit

f. American Registry for Internet Numbers (arin.net)

**Methodology**

19. On February 28, 2025, iDS created a forensic image of the Leviloff Laptop using Cellebrite Digital Collector version 3.8.

20. iDS then processed the forensic image of the Leviloff Laptop using Magnet Forensics' Axiom and mac_apt, both industry-accepted forensic tools for analyzing Mac computers.

21. I then analyzed the forensic artifacts from the Leviloff Laptop, combined with the Google Drive Logs, the Salesforce Login Logs, and the Slack Messages. The findings of my analysis are presented in detail below.

**Analysis**

*Internet History Cleared on the Leviloff Laptop*

22. My analysis showed that the Google Chrome browser ("Chrome") was used on the Leviloff Laptop. Chrome stores, among other things, the history of user visits to websites (URLs), and information about files that users download in a database called "History".

23. On or about February 21, 2025 at 12:56 PM (Eastern), Leviloff's account on the Leviloff Laptop was used to access the URL "chrome://settings/clearBrowserData" in Chrome.

24. My analysis of the "urls table" in the Chrome "History" database showed that the earliest available entry in the table is dated February 21, 2025 at 12:56:31PM (Eastern). The "downloads" table in the same database, however, remains intact.[3]

25. Based on this information, it is my opinion that Leviloff's account on the Leviloff Laptop was used to selectively clear certain Chrome browser history data on or about February 21, 2025 at 12:56 PM (Eastern).

26. While a limited amount of previous browser history was recovered using forensic tools, this clearing of browsing history limited my ability to conduct a full investigation of the websites Leviloff visited, including any visits that may have been made to personal Cloud storage websites such as Google Drive.

*Access to Personal Gmail Account*

27. On February 21, 2025 at 12:57 PM, after browsing history was cleared, Leviloff's laptop was used to access the jXXXXXXXXX@gmail.com Google account.

28. My analysis of the recovered browsing activity showed that Chrome was also used to access the jXXXXXXXXX@gmail.com Google account the day before - February 20, 2025 between 11:52 AM and 2:57 PM (Eastern).

29. Because Chrome browsing history was cleared, it is not possible to determine whether Leviloff's accessed his personal Gmail account or his personal Google Drive account prior to February 20, 2025, nor is it possible to determine what activity, such as composing Gmail emails, accessing specific Gmail emails, or uploading files to the personal Google Drive, occurred prior to February 20, 2025.

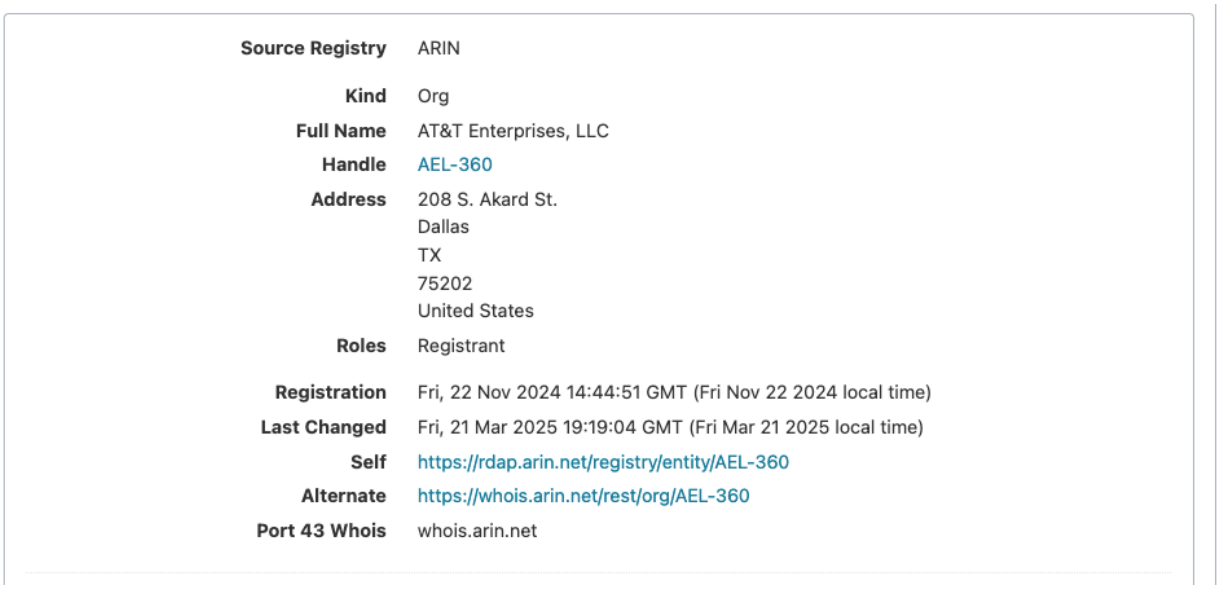
[3] There are 616 records of Chrome download activity available between August 3, 2023 at 3:22:10PM Eastern and February 20, 2025 at 11:45:55 AM Eastern.

*Google Drive Download Activity and Use of Other Devices*

30. I reviewed Google Drive Logs which are available going back to August 28, 2024. My analysis showed that on February 19, 2025, a device connected to Leviloff's account, jleviloff@middesk.com, was used to download a file containing Middesk information ("Middesk Model Validation.pdf "). That device had the IP address **2600:387:c:7013::c**.

31. I analyzed available Chrome download history and did not find evidence of this file downloaded to the Leviloff Laptop on February 19, 2025.

32. I used the American Registry for Internet Numbers (ARIN.net) to check the information recorded about the above IP address and determined that it was assigned to an AT&T wireless customer.[4] A screenshot of the information recorded by ARIN.net is below.



| | |
|---|---|
| **Source Registry** | ARIN |
| **Kind** | Org |
| **Full Name** | AT&T Enterprises, LLC |
| **Handle** | AEL-360 |
| **Address** | 208 S. Akard St.<br>Dallas<br>TX<br>75202<br>United States |
| **Roles** | Registrant |
| **Registration** | Fri, 22 Nov 2024 14:44:51 GMT (Fri Nov 22 2024 local time) |
| **Last Changed** | Fri, 21 Mar 2025 19:19:04 GMT (Fri Mar 21 2025 local time) |
| **Self** | https://rdap.arin.net/registry/entity/AEL-360 |
| **Alternate** | https://whois.arin.net/rest/org/AEL-360 |
| **Port 43 Whois** | whois.arin.net |

*Figure 1. Arin.net results for IP address 2600:387:c:7013::c*

33. Based on my analysis, it is my opinion that the file downloaded on February 19, 2025 by Leviloff's Middesk account from Google Drive was to a device other than the Leviloff Laptop.

[4] https://search.arin.net/rdap/?query=2600%3A387%3Ac%3A7013%3A%3Ac

34. I would need to examine that device to determine the full extent of the download activity, and to understand whether further transfer of this and/or other files occurred from that device.

35. Because Chrome browsing history was cleared on the Leviloff Laptop and because Google Drive Logs only go back to August 28, 2024, there may be other files that were downloaded to other devices that I am not aware of. As such, my analysis related to Google Drive downloads should be considered the floor of download activity, not the ceiling.

*Access to Product & Data Partnerships Tracker File*

36. I was advised that someone within Middesk shared a sensitive document related to Middesk products and partnerships with Leviloff via Slack.

37. My review of the Slack Messages, combined with Google Drive Logs, showed that on February 10, 2025 at 17:42:41 UTC (12:42:41 PM Eastern) user "jpatel" shared a file matching this description with Leviloff.

38. On February 10, 2025 at 12:48:35 PM Eastern, this file was viewed from Google Drive by Leviloff's account jleviloff@middesk.com.

39. I did not find evidence that the Leviloff Laptop was used to view this file.

40. Because of this, and combined with my analysis of synchronization activity described below, it is my opinion that file shared by jpatel on February 10, 2025 was viewed by Leviloff's account on a device other than the Leviloff Laptop.

41. I would need to examine this device to determine the full extent of any transfer or sharing activity

*Google Drive Synchronization Activity and Use of Other Devices*

42. My review of the Google Drive Logs also showed that there was activity for the event "Item content synced". Based on my experience and research, one reason Google Drive Logs record an "Item content synced" event is when "a file is synced to a device for offline access".[5]

43. My analysis showed that on February 20, 2025 in a span of approximately 30 seconds, 38 documents were synchronized between Middesk's Google Drive and a device. I am advised that the documents that were synchronized contain confidential and proprietary Middesk information related to Middesk's pricing, operations, sales, and services.

44. When comparing to the files on the Leviloff Laptop, I did not find all of these 38 files on the Leviloff Laptop. Based on this analysis, it is my opinion that the above-mentioned files were synchronized to a device other than the Leviloff Laptop. It is possible that these files, and other Middesk files, still exist on said device. I would need to examine this device to determine the full extent of synchronization and any transfer or sharing activity.

*Salesforce Activity on the Leviloff Laptop*

45. I understand that Middesk uses Salesforce, a common Customer Relationship Management ("CRM") platform, to keep track of its sales activities. Middesk Salesforce includes, among other things, client information and sales pipeline information.

46. Recovered browsing history on the Leviloff Laptop shows that on or about February 21, 2025 at 10:14 AM, Leviloff's account was used to access Middesk's Salesforce portal.

[5] https://support.google.com/a/answer/4579696?hl=en

47. I also found evidence that Leviloff's account accessed an additional 15 Middesk Salesforce website "pages" using Chrome. These "pages", by page title, appear to be related to Middesk's sales pipeline, pricing, opportunities, and accounts.

48. Because Chrome browsing history was cleared, it is not possible to determine when Leviloff's account accessed the above Salesforce pages or what activity, if any, occurred when the pages were accessed.

*Salesforce Activity on Other Devices*

49. My review of the Salesforce Login Logs showed that beginning on December 5, 2025 and all the way through February 21, 2025, Leviloff's account was used to access Salesforce from an iPhone.

50. While the earliest available date of the Salesforce Login Logs is September 3, 2024, the earliest date of login from an iPhone is December 5, 2024. Other dates of iPhone activity include:

a. January 9, 2025

b. January 14, 2025

c. February 2, 2025

d. February 5, 2025

e. February 21, 2025

51. I understand that it is possible to set up event monitoring in Salesforce, which will track activity, such as page access, edits, and content downloads[6]. I understand that Middesk's instance of Salesforce did not have event monitoring enabled.

[6] https://help.salesforce.com/s/articleView?id=000387928&type=1

52. I would need to analyze the iPhone Leviloff used to access Salesforce to determine the full extent of access, download, transfer, sharing, or screenshot activity that occurred.

*iCloud Drive and Use of Personal Account on Leviloff Laptop*

53. During my analysis, I determined that the Leviloff Laptop was setup to use an Apple ID jXXXXXXXXXXX@yahoo.com. Since this account does not end with "@middesk.com", it is my opinion that this is not a Middesk Apple ID and is more likely a personal Apple ID.

54. One of the features of Mac computers, like the one used by Leviloff at Middesk, is the ability to synchronize files between the Mac computer and other Apple devices using iCloud Drive.[7] The Apple ID is used to access and synchronize iCloud Drive and other Apple services[8].

55. I identified a screenshot on the Leviloff Laptop, taken on January 24, 2025, which indicates iCloud Drive may have been enabled on the Leviloff Laptop at that time.

[7] https://support.apple.com/guide/icloud/icloud-drive-on-icloudcom-overview-mmd0b4a7f5e8/icloud

[8] https://support.apple.com/guide/icloud/apple-account-and-icloud-mm864f5e6593/icloud

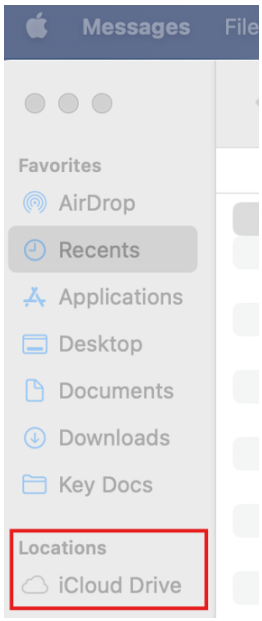



*Figure 2. Crop of Screenshot 2025-01-24 at 10.32.25 AM (2).png*

56. Because the Leviloff Laptop was configured with a personal Apple ID, it is possible that files from the Leviloff Laptop were synchronized to the iCloud account associated with Apple ID jXXXXXXXXXXX@yahoo.com. If the files were not deleted from that iCloud account., it is also possible that anyone with access to the Apple ID jXXXXXXXXXXX@yahoo.com can still access these files.

57. I would need to examine the iCloud account associated with the Apple ID jXXXXXXXXXXX@yahoo.com to determine what, if any, files were synchronized from the Leviloff Laptop to iCloud.

*iMessages and Communications with Jonathan Awad*

58. I found evidence that, until February 6, 2025, the Leviloff Laptop synchronized and stored iMessage communications for Apple ID joshleviloff@yahoo.com.

59. I found evidence of iMessage communications between jXXXXXXXXXXX@yahoo.com and the phone number +1-646-331-5160 for the period January 22, 2025 5:55PM (Eastern) and February 5, 2025 12:56 PM (Eastern). Based on my review of the communications, I

understand that this phone number is associated with Jonathan Awad. Based on my review, I understand that the nature of the communications relate to Leviloff's future employment at Baselayer.

60. Because iMessage communications with Awad end on February 5, 2025 and the last available iMessage communication stored on the Leviloff Laptop is on February 6, 2025, I am unable to determine the full extent of their conversation after this date.

61. I would need to examine the accounts and devices that Leviloff and Awad used to conduct the communications to determine the full extent of their communications including what, if any, Middesk information was shared.

*Inability to access or analyze the Awad Laptop*

62. On March 20, 2025, iDS received the Awad Laptop for forensic imaging and analysis.

63. I determined that the laptop is linked to an Apple ID associated with email address j*****@gmail.com[9]. Because the email address does not end with "@middesk.com", it is my opinion that this is not a Middesk Apple ID and is more likely a personal Apple ID.

64. Without access to this Apple ID, which requires knowing both the full email address and the password, I am unable to access the contents of, create a forensic image of, or analyze the Awad Laptop.

*Additional Access to Devices and Accounts Needed*

65. Based on my analysis to date, I am aware that information relevant to this investigation resides outside of the Leviloff Laptop. In order to complete my investigation and

[9] The email address is obscured on the screen of the Awad Laptop, indicating that the computer is linked to this account. One must type the full email address and password to gain access.

determine the full extent of data copy, transfer or further conveyance of Middesk information, I would need access to at least the following devices and accounts:

a. Leviloff's Google account – jXXXXXXXXX@gmail.com.

b. Leviloff's iCloud account associated with email address jXXXXXXXXXXX@yahoo.com.

c. Leviloff's personal phone.

d. Leviloff's personal computer(s).

e. Leviloff's Baselayer-provided computer.

f. Leviloff's Baselayer-provided email account.

g. Awad's Apple ID associated with email account j*****@gmail.com, including the full email address and password to the same.

h. Awad's device(s) used to communicate with Leviloff.

i. Awad's Baselayer-provided computer.

j. Awad's Baselayer-provided email account.

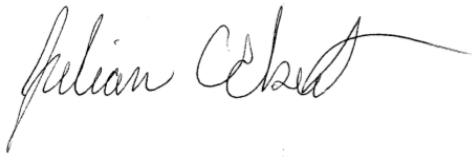
k. Baselayer accounts or systems that Leviloff connected to and/or emailed.

66. Without access to these devices and accounts, my investigation is incomplete.

I reserve the right to supplement or amend these findings and/or opinions should new information become available.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 27th day of March 2025 in Washington, D.C.



Julian Ackert

# JULIAN ACKERT

**Managing Director**

**iDiscovery Solutions, Inc.**

**202.249.7865**

jackert@idsinc.com

Profile on LinkedIn

@iDiscoveryInc

Mr. Julian Ackert, a Managing Director at iDiscovery Solutions (iDS) in Washington DC, has over 20 years of consulting and project management experience in the technology and litigation industries.

He has extensive experience with forensic data collection, computer forensic analysis, creating and implementing preservation and collection strategies, managing electronic data processing and review endeavors, analyzing complex transactional data systems, and working with large multi-national corporations to establish and develop methodologies and best practices for litigation preparedness. Mr. Ackert has written expert reports and provided testimony on the forensic preservation, acquisition, and analysis of electronic information. Additionally, he has worked on several international projects involving complex data privacy, collection, and review challenges.

Mr. Ackert is a member of The Sedona Conference, Working Group 11 (Data Security and Privacy Library) and Working Group 12 (Trade Secrets). Prior to joining iDS, he was a Principal and New York regional lead at LECG and a Manager at FTI Consulting. Mr. Ackert began his career designing, developing, and implementing Knowledge Management / Content Management applications, government middleware solutions, and E-business applications for Federal Government services at Accenture.

## SELECT CONSULTING EXPERIENCE

- Directed a team of consultants on the identification, preservation, collection and production of structured data for an antitrust MDL. Implemented custom preservation and collection protocols and extracted approximately 10 terabytes of structured data from proprietary client database systems for analysis and review. Developed a structured data ESI protocol that governed the parameters of structured data productions.
- Managed a team of consultants on the analysis of 100s of millions of database records for a complex ligation in the commercial real estate industry. Analyzed trends and patterns in the database records that assisted counsel with identifying potentially relevant employees, partner relationships, and timeframes of interest.
- Managed a team of UK and US consultants on a data preservation and email data analysis endeavor. Established an onsite review room in the UK and worked with UK outside counsel to ensure that electronic discovery processes upheld EU data privacy laws.
- Directed a team of computer forensic consultants and contractors on forensic data preservation, backup tape recovery, email, and electronic file culling and search for approximately 100 custodians. Established an onsite triage center at an offshore facility to handle nearly 5 terabytes of data. Authored expert report on the methods, processes, types, and volumes of data preserved, processed, and delivered for attorney review.
- Led a data analysis engagement consisting of metadata examination on Lotus Notes database documents. Acted as the client's Subject Matter Expert on Lotus Notes databases and authored expert testimony on the electronic discovery methods implemented during the project and subsequent project findings.
- Managed investigative team of computer forensic and complex data analysis consultants through the preservation, acquisition, and analysis of over 5 billion rows of NYSE trade data. Analysis period covered over 5 years of transactional data focusing on the alleged fraudulent trading activity.
- Managed a data acquisition, e-file processing, and document review project in response to an SEC inquiry of over 45 custodians. Engagement required leading a multi-city team of computer forensic professionals through the forensic acquisition, electronic data processing, and document review phase of a project with a condensed project timeline of three weeks.
- Led multi-national electronic discovery preservation and analysis team on an internal audit committee investigation of a global metallurgy company. Engagement required managing computer forensic technicians through data preservation, forensic analysis, and automated culling of both Finnish and English enterprise email, financial data, and business documents related to the investigation.

## EDUCATION

- University of Virginia, Charlottesville, VA
- School of Engineering and Applied Sciences
- B.S. Computer Science, January 1998

## SELECT PUBLICATIONS

- "GDPR and Data Maps: "X" Marks the Spot to Delete", Today's General Counsel, July 2018
- "5 Tips to Help Mitigate Insider Theft", Metropolitan Corporate Counsel, March 2017
- "A Practical Approach to Data Preservation and Collection", Metropolitan Corporate Counsel, May 2015
- "Big Data: The Elephant in The E-Discovery Room", Metropolitan Corporate Counsel, June 2013

## TESTIFYING EXPERIENCE

1. Expert Report on computer forensic and metadata analysis, DB Home Designs, LLC d/b/a EKB Kitchens v. Matthew Wilhelm, Leah Russo, Stephanie Hendricks, and Emmco Kitchens, Inc., December 2024.
2. Declaration on computer forensic analysis activities, G&P Group Inc. v. City National Bank, November 2024.
3. Trial Testimony on computer forensic and metadata analysis, Robin Greenwood, Senior Associate Dean for Faculty Development and Research v. Francesca Gino, Professor of Business Administration, November 2024.
4. Deposition on computer forensic analysis activities, Sunrgy, LLC v. SolarTek, Inc., October 2024.
5. Expert Report on computer forensic and metadata analysis, Sunrgy, LLC v. SolarTek, Inc., September 2024.
6. Expert Statement on computer forensic and metadata analysis, Robin Greenwood, Senior Associate Dean for Faculty Development and Research v. Francesca Gino, Professor of Business Administration, September 2024.
7. Expert Report on computer forensic and metadata analysis, Potomac Wave Consulting, Inc. v. Robert Harford, September, 2024.
8. Deposition on computer forensic analysis activities, Madison Joint Ventures, LLC v. Chemo Research S.L. Exeltis USA, Inc. and Sergio Sosa-Estani, July 2024.
9. Expert Report on computer forensic and metadata analysis, Maximus, Inc. v. Alyssha Holdren, July 2024.
10. Declaration on computer forensic analysis activities, Madison Joint Ventures, LLC v. Chemo Research S.L. Exeltis USA, Inc. and Sergio Sosa-Estani, May 2024.
11. Declaration on computer forensic analysis activities, Potomac Wave Consulting, Inc. v. Robert Harford, May, 2024.
12. Declaration on forensic data analysis activities, In re: Isaac Halwani and Giselle Halwani and 274 Atlantic Isles, LLC, May 2024
13. Declaration on forensic data analysis activities, Linda Johnstone v. CrossCountryMortgage, LLC, April 2024
14. Declaration on forensic data analysis activities, In re: Isaac Halwani and Giselle Halwani and 274 Atlantic Isles, LLC, April 2024
15. Declaration on forensic data analysis activities, Finch Computing Corp. v. Joseph Cirka, March 2024
16. Declaration on computer forensic data analysis activities, Tyrone Brewer v. Pepperidge Farm, Inc., March 2024
17. Declaration on forensic data analysis activities, Maximus, Inc. v. Alyssha Holdren, March 2024
18. Declaration on ESI review and production effort, State of Maryland v. Monsanto Company, et. al., March 2024
19. Declaration on forensic data analysis activities, Linda Johnstone v. CrossCountryMortgage, LLC, March 2024
20. Declaration on ESI review and production effort, Michael Krantz, et. al. v. Regeneron Pharmaceuticals, Inc. and Sanofi Aventis US, LLC, February 2024
21. Declaration on computer forensic analysis activities, Nicholas Hall v. Steve Eakin, Robert Taylor, Scott Brown, T3 Holdings Group, LLC and Michelle Taylor, February 2024
22. Declaration on computer forensic data analysis activities, Tyrone Brewer v. Pepperidge Farm, Inc., February 2024
23. Declaration on computer forensic data analysis activities, Tyrone Brewer v. Pepperidge Farm, Inc. January 2024
24. Deposition on computer forensic analysis activities, Pacmar Technologies, LLC v. Goodsill Anderson Quinn & Stifel LLP et. al, January 2024
25. Declaration on computer forensic analysis activities, The Crème Shop, Inc. v. Sunna ("Olive") Kim, et. al., November 2023
26. Affidavit on computer forensic analysis activities, Spartan Medical Inc. v. Erik Gottschalk, November 2023

27. Declaration on computer forensic analysis activities, RF Depot Inc. v. Richard H. Pouliot and Applied Specialties, inc., August 2023
28. Declaration on computer forensic analysis activities, James Michael Richey v. Nevro Corp., July 2023
29. Declaration on computer forensic and metadata analysis, Alcon Inc. et. al. v. Hoya Corporation, et. al., June 2023
30. Declaration on forensic data analysis activities, Maria Fernanda Soto Leigue v. Everglades College, Inc. d/b/a Keiser University, May 2023
31. Declaration on computer forensic analysis activities, IOENGINE, LLC v. Roku, Inc., May 2023
32. Expert Report on computer forensic and metadata analysis, USA v. David Gerald Minkkinen, Sivaraman Sambasivam, May, 2023
33. Declaration on computer forensic analysis activities, Galderma Laboratories, L.P., v. Chad Tiscкos, April 2023
34. Declaration on forensic data analysis activities, Maria Fernanda Soto Leigue v. Everglades College, Inc. d/b/a Keiser University, February 2023
35. Declaration on computer forensic analysis activities, Dollar Shave Club, Inc., and Michael O'Malley v. Edgewell Personal Care Company, et. al., November 2022
36. Declaration on computer forensic analysis activities, CACI, Inc. – Federal v. Clayton Shcilling, et. al., September 2022
37. Trial Testimony on computer forensic analysis activities, Medidata Solutions, Inc. and MDSOL Europe Limited v. Veeva Systems, Inc., July 2022
38. Declaration on ESI review and production effort, Joseph Bayer, Mary K. Bayer, and Gwendolyn Culverson v. Boehringer Ingelheim Pharmaceuticals, Inc. et. al., July 2022
39. Declaration on ESI search and production protocols, Trust-ED Solutions, LLC v. Gilbert, LLP, June 2022
40. Trial Testimony on computer forensic analysis activities, John C. Depp, II, v. Amber Laura Heard, May 2022
41. Deposition on computer forensic analysis activities, Icertis, Inc. v. Boccella, et al. May 2022
42. Expert report on computer forensic analysis activities, Icertis, Inc. v. Boccella, et al. May 2022
43. Declaration on computer forensic analysis activities, Julius Kennedy and Angela Kennedy v. Heding Truck Service Inc. et. al., April 2022
44. Deposition on computer forensic analysis activities, John C. Depp, II, v. Amber Laura Heard, April 2022
45. Expert report on computer forensic analysis activities, John C. Depp, II, v. Amber Laura Heard, April 2022
46. Supplemental expert report on forensic data analysis activities, Megan Enger and Sarah Infante. v. Thomas L. Cardella & Associates, April 2022
47. Declaration on computer forensic analysis activities, Dollar Shave Club, Inc. et. al. v. Edgewell Personal Care Company et. al., April 2022
48. Deposition on forensic data analysis activities, Megan Enger and Sarah Infante. v. Thomas L. Cardella & Associates, April 2022
49. Deposition on computer forensic analysis activities, Chi Nguyen v. City of Philadelphia, March 2022
50. Declaration on computer forensic analysis activities, BDO USA LLP v. Everglade Global Inc., February 2022
51. Deposition on computer forensic analysis activities, BDO USA LLP v. Everglade Global Inc., January 2022
52. Declaration on computer forensic analysis activities, Gilead Tenofovir Cases, JCCP No. 5043, December 2021
53. Declaration on computer forensic analysis activities, Michael David Testa, Individually and as Trustee of The M. David Testa Revocable Living Trust, Dated October 25, 2017 v. Town of Jupiter Island, December 2021
54. Expert report on forensic data analysis activities, Megan Enger and Sarah Infante. v. Thomas L. Cardella & Associates, November 2021
55. Declaration on collection and production of social media, In Re: Zantac (Ranitidine) Products Liability Litigation, November 2021
56. Declaration on computer forensic analysis activities, Chi Nguyen v. City of Philadelphia, October 2021
57. Declaration on computer forensic analysis activities, John C. Depp, II, v. Amber Laura Heard, October 2021
58. Declaration on computer forensic analysis activities, Marley R. Dominguez v. Iconiq Capital Management, LLC, October 2021

59. Declarartion on computer forensic analysis activities, Sunlight Financial LLC, and Sunlight Financial Holdings, Inc. v. Duncan Hinkle, and Sunstone Credit, Inc., August 2021
60. Declaration on ESI search and production, Gilead Tenofovir Cases, JCCP No. 5043, July 2021
61. Deposition on forensic data analysis activities, Lainhart et. al. and Doyle et. al. v. Louisville/Jefferson County Metro Government, July 2021
62. Expert report on forensic data analysis activities, Lainhart et. al. and Doyle et. al. v. Louisville/Jefferson County Metro Government, June 2021
63. Deposition on computer forensic analysis activities, Havana Docs Corporation v. Carnival Corporation d/b/a Carnival Cruise Line, June 2021
64. Declaration on computer forensic analysis activities, eHealthInsurance Services, Inc. v. Healthpiolt Technologies LLC., May 2021
65. Declaration on computer forensic analysis activities and spoliation issues, Medidata Solutions, Inc. and MDSOL Europe Limited v. Veeva Systems, Inc., April 2021
66. Declaration on computer forensic analysis activities, Havana Docs Corporation v. Carnival Corporation d/b/a Carnival Cruise Line, March 2021
67. Court Testimony on computer forensic analysis activities, State of Maryland v. Darrian McAfee
68. Expert report on forensic data analysis activities, Kaelin et. al. v. Louisville/Jefferson County Metro Government, January 2021
69. Declaration on computer forensic analysis activities, Sequoia Benefits & Insurance Services DBA Sequoia Consulting Group v. Sageview Advisory Group et. al., January 2021
70. Declaration on computer forensic analysis activities, Doneyda Perez v. DirectTV Group Holdings LLC, et al., December 2020
71. Declaration on ESI search and production protocols, Trust-ED Solutions, LLC v. Gilbert, LLP, November 2020
72. Declaration on computer forensic analysis activities, Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc. and Chris Conrad, November 2020
73. Declaration on ESI review and production effort, Gilead Tenofovir Cases, JCCP No. 5043, August 2020
74. Declaration on collection and production of social media, Adrian Holley, et al. v. Gilead Sciences, Inc., August 2020
75. Declaration on collection and production of social media, Gilead Tenofovir Cases, JCCP No. 5043, July 2020
76. Declaration on computer forensic analysis activities, Doneyda Perez v. DirectTV Group Holdings LLC, et al., July 2020
77. Expert report on forensic data analysis activities, Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc. and Chris Conrad, June 2020
78. Declaration on ESI review and production effort, Adrian Holley, et al. v. Gilead Sciences, Inc., May 2020
79. Declaration on ESI production protocols, Adrian Holley, et al. v. Gilead Sciences, Inc., April 2020
80. Declaration on computer forensic analysis activities, Krista Brill v. Draeger, Inc. and Miguel Angel Armendariz, April 2020
81. Deposition on computer forensic analysis activities, Medidata Solutions, Inc. and MDSOL Europe Limited v. Veeva Systems, Inc., April 2020
82. Trial Testimony on computer forensic analysis activities, Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc. and Chris Conrad, March 2020
83. Declaration on computer forensic analysis activities, Jesus Jiminez v. CRC Property Management West, Inc., March 2020
84. Declaration on computer forensic analysis activities, Denver Cooley v. Solar Turbines Incorporated, February 2020
85. Supplemental expert report on forensic data analysis activities, Medidata Solutions, Inc. and MDSOL Europe Limited v. Veeva Systems, Inc., February 2020

86. Declaration on ESI data types, Anthony Robles, Individually and on Behalf of Other Persons Simi-larly Situated v. The Coca-Cola Company, Coca-Cola Refreshments USA, Inc., and Does 1-10, February 2020
87. Declaration on computer forensic analysis activities, Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc. and Chris Conrad, January 2020
88. Expert report on forensic data analysis activities, Medidata Solutions, Inc. and MDSOL Eu-rope Limited v. Veeva Systems, Inc., January 2020
89. Declaration on ESI collection and production effort, Kristopher Lawson, Vincent McCleery, and Sean McMurran, Individually and on Behalf of Other Persons Similarly Situated v. Love's Travel Stops & Country Stores, Inc., December 2019
90. Declaration on ESI review and production effort, Sandra Wolford et. al. v. Bayer Corp. et. al., De-cember 2019
91. Declaration on ESI systems and data recovery options, In the Matter of Certain Lithium Batteries, Battery Cells, Battery Modules, Battery Packs, Components Thereof, and Processes Thereof, Oc-tober 2019
92. Trial Testimony on computer forensic analysis activities, Futrend Technology Inc. v. Microhealth LLC, et. al., October 2019
93. Supplemental expert report on forensic data analysis activities, Futrend Technology Inc. v. Microhealth LLC, et. al., October 2019
94. Declaration on collection, search, and disposition process, Strategic Delivery Solutions, LLC v. Stallion Express, LLC, September 2019
95. Expert report on forensic data analysis activities, Futrend Technology Inc. v. Microhealth LLC, et. al., July 2019
96. Declaration on social media e-Discovery, Helen McLaughlin v. Bayer Essure Inc, et. al., May 2019
97. Declaration on ESI collection and search scoping, Sandra Wolford et. al. v. Bayer Corp. et. al., May 2019
98. Declaration on computer forensic analysis activities, Employee Benefit Services of Maryland, Inc. v. Nicholas Mafale, May 2019
99. Declaration on collection activities, IQVIA Inc. et. al. v. Veeva Systems, Inc., May 2019
100. Declaration on ESI collection and search scoping, Sandra Wolford et. al. v. Bayer Corp. et. al., April 2019
101. Declaration on production activities, Synchronisys, Inc. v. DataSync, Inc. et. al., February 2019
102. Declaration on collection and production activities, Catalus Capital USVI, LLC et. al. v. The Service-master Company, LLC, et. al., January 2019
103. Declaration on collection and search protocols, Strategic Delivery Solutions, LLC v. Stallion Ex-press, LLC, December 2018
104. Expert Report on computer forensic analysis activities, Quandra Speights v. The Boeing Company, December 2018
105. Affidavit on computer forensic analysis activities, Futrend Technology Inc. v. Microhealth LLC et. al., October 2018
106. Affidavit on preservation, collection and search protocols, Sarah Lankford Sprecher v. Leroy E. My-ers, Jr., September 2018
107. Declaration on computer forensic analysis activities, Yifat Oren et. al, v. Stefanie Cove, et. al., Au-gust 2018
108. Trial Testimony on metadata and computer forensic analysis activities, Broadcast Sports Interna-tional, LLC v. Gil Pascal, et. al., June 2018
109. Declaration on computer forensic analysis activities, Airgas, Inc. v. The Carlyle Group, Carlyle In-vestment Management, LLC, and Leslie Graff, June 2018
110. Supplemental Declaration on e-Discovery deduplication and production protocols, Helen McLaughlin v. Bayer Essure Inc, et. al., May 2018
111. Declaration on computer forensic analysis activities, Charlotte Pinckney and Kyle Pinckney v. The Pep Boys Manny Moe & Jack O/D/B/A Pep Boys, May 2018

112. Declaration on e-Discovery deduplication and production protocols, Helen McLaughlin v. Bayer Essure Inc, et. al., March 2018
113. Declaration on e-Discovery deduplication and production protocols, Hannah Dorman et. al. v. Bayer, Corp, et. al., February 2018
114. Court Testimony on computer forensic analysis activities, MRP UO Partners, LLC, et. al, v. Ray-mond Rahbar, Jr. et. al., October 2017 – November 2017
115. Deposition on computer forensic analysis activities, MRP UO Partners, LLC, et. al, v. Raymond Rahbar, Jr. et. al., September 2017
116. Declaration on computer forensic analysis activities, MRP UO Partners, LLC, et. al, v. Raymond Rahbar, Jr. et. al., August 2017
117. Deposition on computer forensic analysis activities, Broadcast Sports International, LLC v. Gil Pas-cal, et. al., July 2017
118. Declaration on computer forensic analysis activities, Meridian Imaging Solutions, Inc. et. al. v. Om-ni Business Solutions LLC, et. al., July 2017
119. Declaration on computer forensic analysis activities, Yadkin Bank v. George Mason Mortgage, Inc. et. al, June 2017
120. Declaration on computer forensic analysis activities, Nichole Baibos v. ConnectYourCare LLC, May 2017
121. Expert report on forensic data analysis activities, Broadcast Sports International, LLC v. Gil Pascal, et. al., April 2017
122. Declaration on preservation and collection protocols, MD Helicopters, Inc. v. Aerometals, Inc., April 2017
123. Affidavit on computer forensic analysis activities, Yadkin Bank v. George Mason Mortgage, Inc. et. al, March, 2017
124. Court Testimony on metadata and computer forensic analysis activities, George Mason Mortgage, Inc. v. Caliber Home Loans, Inc., February 2017
125. Deposition on computer forensic analysis and deletion activities, Medidata Solutions, Inc. v. Michael Petrarca and Bioclinica, Inc., November 2016
126. Expert Rebuttal Report on data breach analysis, Employment Background Investigations, Inc. v. Federal Insurance Company, October 2016
127. Expert Report on data breach analysis, Employment Background Investigations, Inc. v. Federal In-surance Company, July 2016
128. Affidavit on computer forensic analysis activities, Compass Systems, Inc. v. Frank D. Deaton, July 2016
129. Affidavit on computer forensic analysis activities, Broadcast Sports International, LLC v. Gil Pascal, et. al., June 2016
130. Affidavit on forensic analysis and data recovery, Felicia M. Barlow Clar et. al, v. Kyle C. Muehlhauser, et. al, May 2016
131. Affidavit on preservation and collection protocols, IN RE: Blue Cross Blue Shield Antitrust Litiga-tion, December 2015
132. Affidavit and Court Testimony on computer forensic analysis activities, Stradtman v. Republic Ser-vices, Inc., May 2015
133. Expert report and Deposition on metadata and forensic data analysis activities, Headfirst Baseball LLC, et. al., v. Robert Elwood, et al., May 2015
134. Expert report and Deposition on metadata and forensic data analysis activities, Integrated Direct Marketing, LLC v. Drew May and Merkle, Inc., April 2015
135. Expert report on metadata and forensic data analysis activities, George Mason Mortgage, Inc. v. Caliber Home Loans, Inc. et al., April 2015

## SELECT SPEAKING ENGAGEMENTS AND CONFERENCES

1. Sedona Conference Working Group 11 – "Biometric Privacy Primer", October 2021
2. Sedona Conference Working Group 11 – "Artificial Intelligence (AI) model transparency: Core principles in promoting transparency of AI and algorithms", October 2019
3. Sedona Conference Working Group 11 – "Data Security and Privacy Legal issues in Artificial Intel-ligence", March 2018
4. Webinar, Metropolitan Corporate Counsel – "Data Breach Response: Orchestrating Legal & Tech-nical Resources to Contain & Mitigate", March 2017
5. Sedona Conference Working Group 11 – "Privacy by Design", St. Petersburg, January 2017
6. CLE, ZwillGen, Cloud Computing and Mobile Devices, November 2016
7. Sedona Conference Working Group 11 – "Privacy by Design", Seattle, August 2016
8. The Exchange (Today's General Counsel Institute) – "Strategic Use of Objections and Responses Under New Rule 34", Chicago, June 2016
9. CLE Panel, "Engaging and Managing the Presentation and Preparation of Expert Witnesses in Bankruptcy and Federal Court", May 2016
10. CLE Webinar, The Knowledge Group – "Mobile Data and BYOD: Mitigating eDiscovery and Data Breach Risks", April 2016
11. CLE Webinar, The Knowledge Group – "Mobile Privacy and Security Issues in 2015: Practical Guid-ance to Mitigate Data Breaches", August 2015
12. The Exchange (Today's General Counsel Institute) - "The Importance of Project and Process Man-agement", Chicago, June 2015
13. Masters Conference - "Cloud Computing and Mobile Devices – How to Be Prepared for Litigation", Philadelphia, July 2014
14. The Exchange (Today's General Counsel Institute) - "The 'eWorkplace' and its Impact on eDiscov-ery", New York, July 2014
15. Masters Conference - "Discussion and Debate Over Potential Changes to the Federal Rules of Civ-il Procedure", Chicago, May 2014
16. Masters Conference, "Predictive Analytics and Its Effect on Big Data", Chicago, May 2014
17. Chicago Association of Litigation Support Managers (CALSM-posium), "Forensic Collection Trends Now and into the Near Future", October 2013
18. CLE, Tydings & Rosenberg LLP, "E-Discovery Primer", October 2013
19. Masters Conference, "Cloud Computing and Mobile Device Usage: Challenges They Bring to Your Litigation", July 2013
20. CLE, Williams & Connolly LLP, "Mobile Forensics for Lawyers", January 2013
21. Chicago Association of Litigation Support Managers (CALSM-posium), "How to Prepare for E-Discovery Supplementation Obligations", October 2012
22. Paraben Forensic Innovations Conference, "Analyzing Structured Data", November 2010

## PROFESSIONAL AFFILIATIONS

- The Sedona Conference, Working Group 11 (Data Security and Privacy)
- The Sedona Conference, Working Group 12 (Trade Secrets)